Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
Фізико-технічний інститут

КРИПТОГРАФІЯ

КОМП'ЮТЕРНИЙ ПРАКТИКУМ №2

Криптоаналіз шифру Віженера.

Варіант – 3

Виконали:

студенти III курсу ФТІ групи ФБ-96
Шидлюх Максим та Шафрай Ілля

Мета роботи:

Засвоєння методів частотного криптоаналізу. Здобуття навичок роботи та аналізу потокових шифрів гамування адитивного типу на прикладі шифру Віженера.

Порядок виконання роботи:

0. Уважно прочитати методичні вказівки до виконання комп'ютерного практикуму.
1. Самостійно підібрати текст для шифрування (2-3 кб) та ключі довжини r = 2, 3, 4, 5, а також довжини 10-20 знаків. Зашифрувати обраний відкритий текст шифром Віженера з цими ключами.
2. Підрахувати індекси відповідності для відкритого тексту та всіх одержаних шифртекстів і порівняти їх значення.
3. Використовуючи наведені теоретичні відомості, розшифрувати наданий шифртекст (згідно свого номеру варіанта).

Хід роботи

Завдання 1

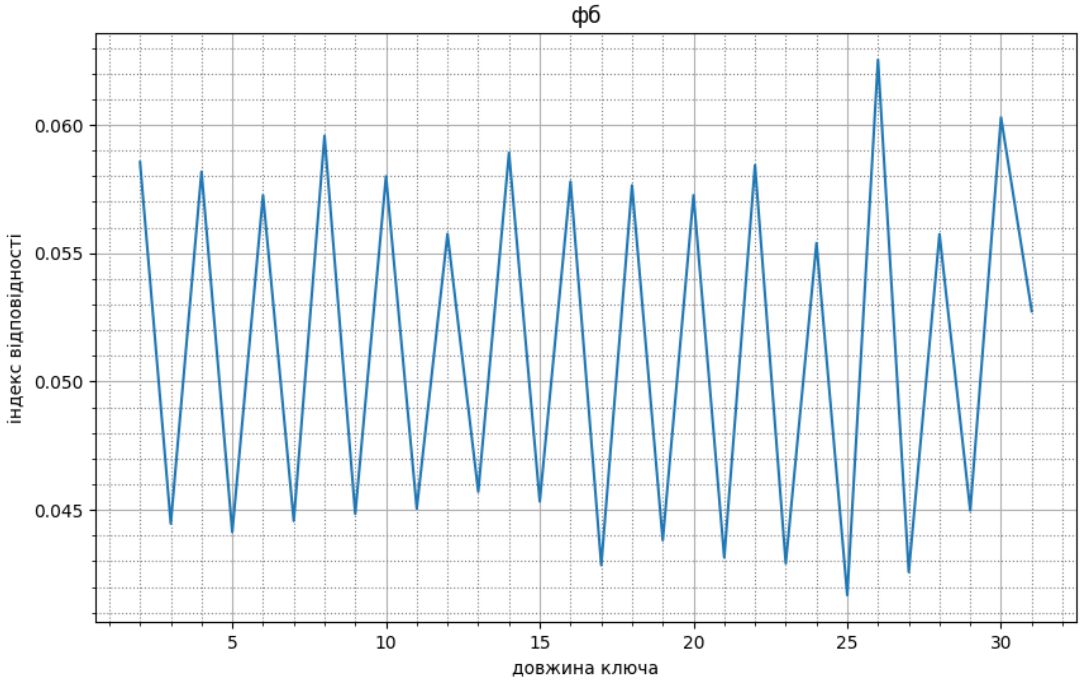
Створення функції шифрації тексту не викликало ніяких перешкод, однак знаходження самого тексту і створення з нього зручного тексту для шифрування було проблематичним. Тому було взято курс на «приборкання» цього тексту силою:

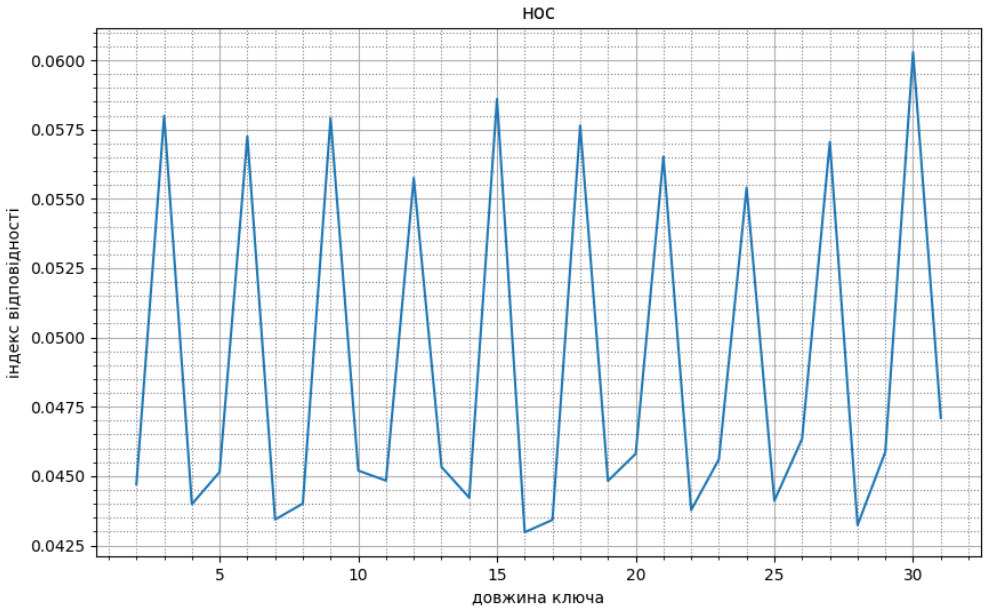
```
VT = file.read().lower().replace("ё", "е").replace(" ", "").replace("!", "").replace(",", "").replace(".", "")\
    .replace("—","").replace(";","").replace(":","").replace("\n","").replace("-","")
```

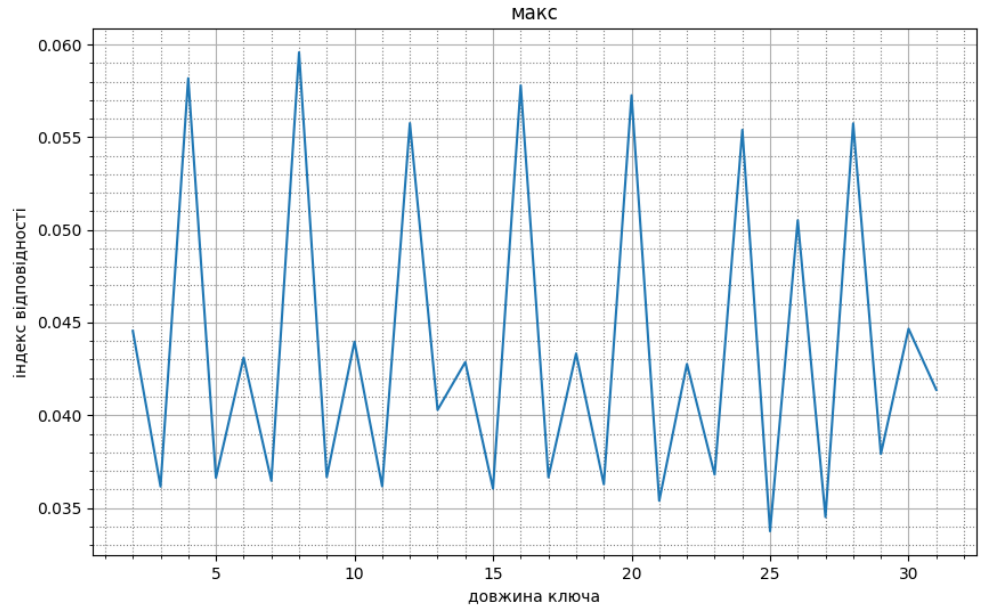
Не найрозумніший підхід, але простий як пробка.

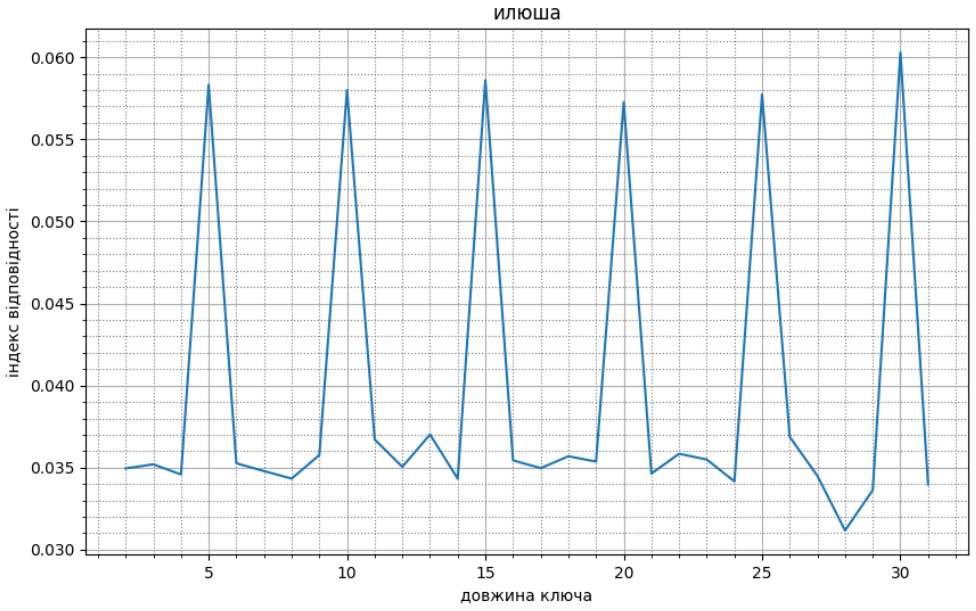
Завдання 2

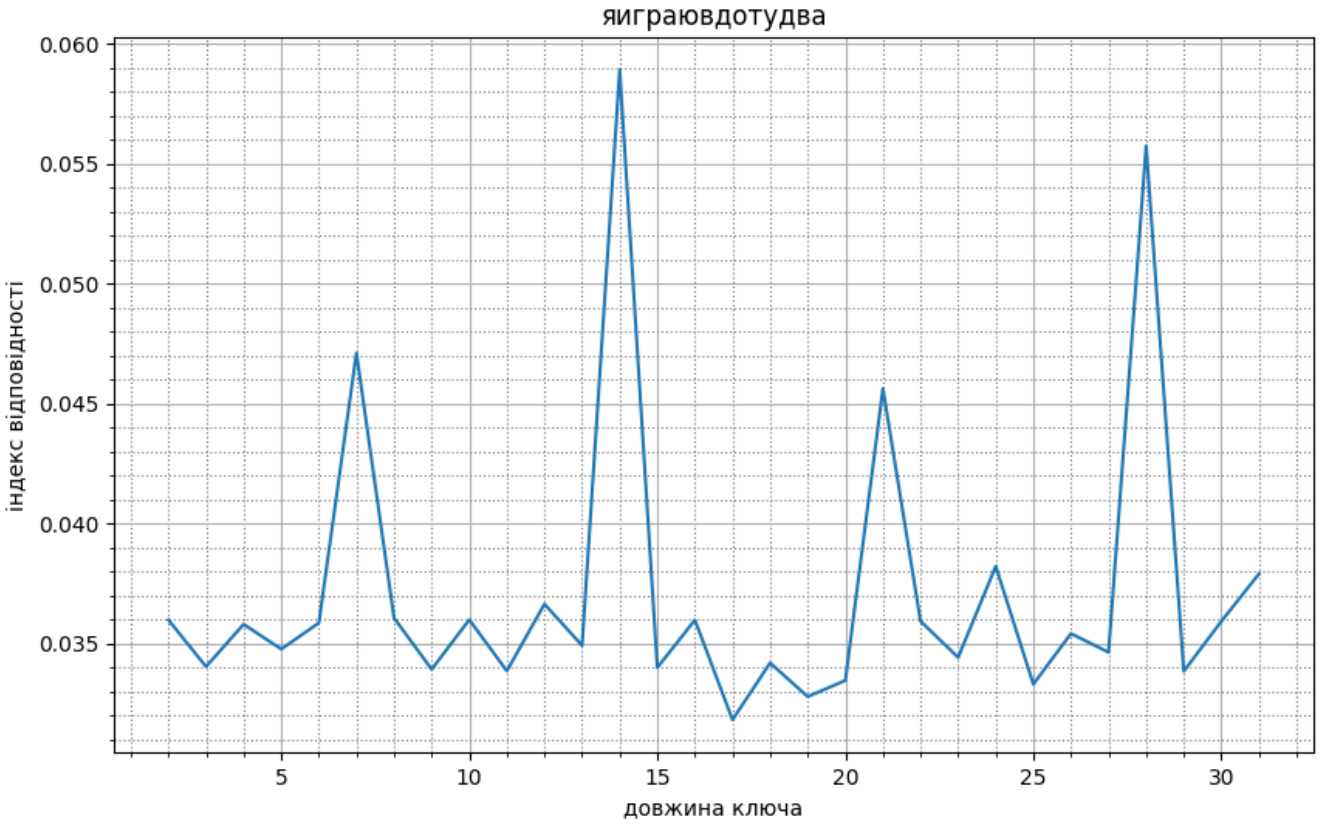
Через неповноцінне виконання Завдання 0 виникло непорозуміння знаходженням Індексу Відповідності, але використання методичних матеріалів дало змогу дотримуватись правильного маршруту роботи.




нос
0.0600
0.0575
0.0550
0.0525
0.0500
0.0475
0.0450
0.0425
індекс відповідності
5
10
15
20
25
30
довжина ключа


макс
0.060
0.055
0.050
0.045
0.040
0.035
індекс відповідності
5
10
15
20
25
30
довжина ключа

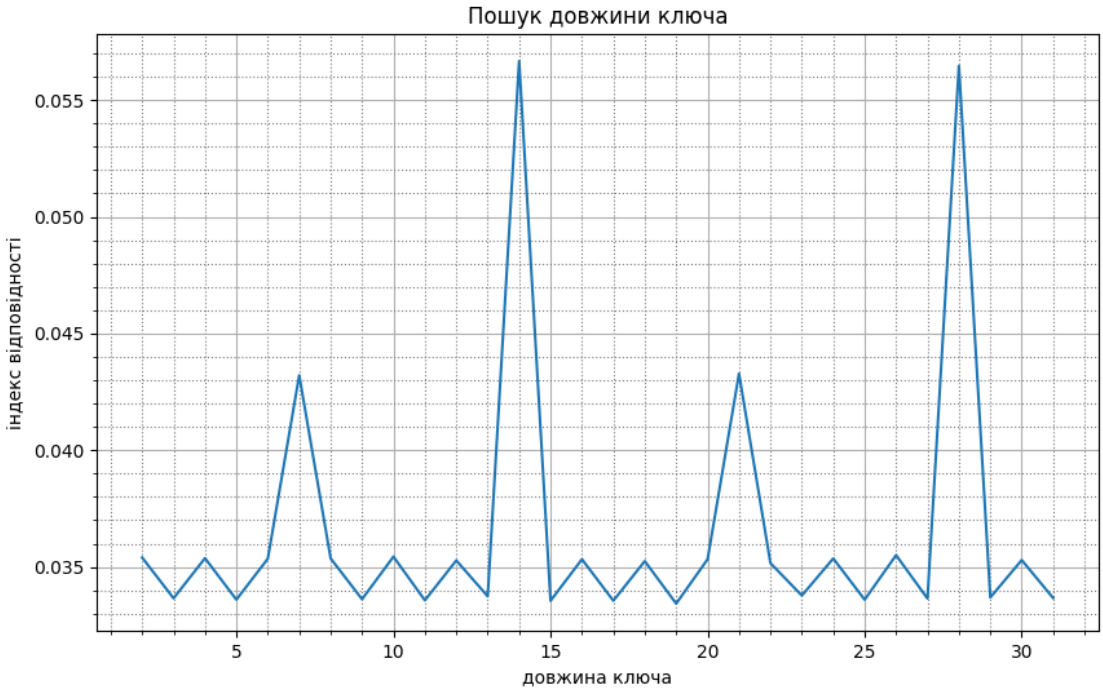

илюша
0.060
0.055
0.050
0.045
0.040
0.035
0.030
індекс відповідності
5
10
15
20
25
30
довжина ключа



Для кожної довжини ключа бачимо, що індекс відповідності найбільший для значення довжини ключа або кратного йому. Таким способом легко визначити довжину ключа шифротексту

Завдання 3

Шукаємо довжину ключа



По графіку видно, що індекс відповідності 14 або 28.
28 ділиться націло на 14, отже ключ має довжину 14

```
0.05667060702875399 : 14
```

Програма обирає найбільше значення індексу відповідності і виводить відповідну йому довжину ключа.

Ділимо текст на блоки в кількості довжини нашого ключа і шукаємо найпопулярніші символи в кожному блоці:

```
['л', 'п', 'ь', 'ъ', 'о', 'д', 'а', 'ы', 'ц', 'ш', 'в', 'б', 'к', 'ь']
```

Припускаючи, що найпопулярнішою буквою у кожному блоці буде «О» (що статистично дуже ймовірно), дешифруємо ключ: эбомацтникфуьо

```
эбомацтникфуьо
```

У трьох блоках ми помилились з припущенням, але вже можемо замінити наш ключ на осмислений його варіант: экомаятникфуко

```
экомаятникфуко
```

Розшифровуємо текст нашим ключем:

→

итутяувиделмаятникшарвисящийнадолгойнитиопущеннойсвольтыхоравизохронномвели чииописывалколебанияязналноивсякийощутилбыподчарамимернойпульсациичтопериодк олебанийопределенотношениемквадратногокорнядлинынитикчислуркотороеиррациональ ноедляподлунныхумовпредлицомбожественнойрационеукоснительносопрягаетокружност исдиаметрамилюбыхсуществующихкруговкакивремяперемещенияшараотодногополюсакп ротивоположномупредставляетрезультаттайнойсоотнесенностинаиболеевневременныхмер единственноститочкикрепленияздвойственностиабстрактногоизмерениятроичностичислап искрытойчетверичностиквадратногокорнясовершенствакругаещеязналчтонаконцеотвесно йлинииивосстановленнойотточкикрепленияснаходящийсяподмаятникоммагнитныйстабилиз аторвоссылаеткомандыжелезномусердцушараиобеспечиваетвечностьдвиженияэтохитраяш тукаимеющаяцельюпереборотьсопротивлениематериинокотораянепротиворечитзаконуфу конапротивпомогаетемупроявитьсяпотомучтопомещенныйвпустотулюбойточечныйвеспр иложенныйкконцунерастяжимойиневесомойнитиневстречающийнисопротивлениявоздуха нитрениявточкекрепленияздействительнобудетсовершатьрегулярныеигармоничныеколеба ниявечномедныйшарпоигрывалбледнымипереливчатымиотблескамиподпоследнимилучам ишедшимиизвитражаеслибыкаккогдатоонкасалсяслоямокрогопесканаплитахполаприкажд омизегокасанийпрочерчивалсябыштрихиэтиштрихинеуловимоизменяякаждыйразнаправле ниерасходилисьбыоткрываяразломытраншеирвыиугадывалась бырадиальнаясимметричнос тькостякмандалыневидимаясхемапентакулазвездымистическойрозынетнетэтобылабынеро заэтобылбырассказзаписанныйнаполотнахпустыниследаминесосчитанныхкарабановповес тьотысячелетнихскитанияхнаверноеэтойдорогойшлиатлантыконтинентамувугрюмойупор нойрешительностиизтасманиивгренландиюотропикакозерогактропикуракасостровапринц аэдуарданашпицбергенкасаниямишараутрамбовывалосьвминутныйрассказвсечтоонитвори ливпромежуткахотодноголедовогопериодадодругогоискореевсеготворятвнашевремясдела вшисьрабамиверховниковвероятноперелетаяотсамоанановуюземлюэтотшарнацеливаетсяв апогеепараболынаагартуцентрмираячувствовалкактаинственнымобщимпланомобъединяет сяавалонгипербореевсполуденнойпустынейоберегающейзагадкуайерсроквданныймигвчет ыречасаднядвадцатьтретьегоиюнямаятникутрачивалскоростьукраяколебательнойплоскост ибезвольноотшатывалсяснованачиналускорятьсякцентруинаразгонепосерединерассекалсс абельнымсвистомтайныйчетвероугольниксилопределявшихегосудьбуеслибыяпробылтамд олгонеуязвимыйдлявременинаблюдаякакэптичьяголоваэтоткопейныйнаконечникэтотоп рокинутыйгребеньшлемавычерчиваетв…

→

Приводити повий текст не бачу сенсу, вже з перших рядків видно, що усі символи розшифровані правильно, особливо побачивши шифротекст:

→

еьбюятфхмпяякнпчццшявпрыумтчкктълвацхтжышэргущнныюкшяпьйтшюмвзщыэъвач
ьймучицъхцщьдерэхшълдунхтутс
ыэхыъибгмттэбгбптщныоасякдуццйпющоибаужеуацебаъпдвхцоюбхуюкыфйнбэнощюп
ылььъшдяхнцюхктнкащовачцъб
тощечйщисъчятеюэюзшаърнчхшъфйтьккщиннчсуйгбощрчызхтюыкщдшощеаьшбнштщ
ьцшчылуюмцзаънэюбыыеьучьма
юцщдтновььцртшъцыжыытекъстптщрхтфегоэзсссфажгьифюрньокяьхкъщяйэвъушешчъ
рймуъолььрннхычшясыозщюътз
фычшябрылцбырдцюъкцюйупъууукояиьжууылуяъосятщпбашяптымиаашнпцапрнпъсн
мнвфпдшоцкыаоемяыщььешезтш
ьеоэтхтучмьжыаоемяыщььуляпъоцтмарцтыяпювчцлтпахячвдьцфтячаоъютъпешчфпаое
пъдхшеетшяктьасяылшюбъыььыо
епктхыжхкшнэсмешчмпчфюбалчоцомитцьцшыылущфнзъпцыеекылмщснмаццьжббшеф
юспкчърйбуяьбйзфйрсьцоауйакт

→

Висновок

Отримали навички у використанні методів частотного криптоаналізу. Систематизували навички роботи та аналізу потокових шифрів гамування адитивного типу на прикладі шифру Віженера. Здобули теоритичні знання, що були поданні у методичних вказівках до Лабораторної роботи №2. Навчилися здорово використовувати деякі можливості бібліотек matplotlib і collections.